(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－202484
（P2001－202484A）
(43)公開日　平成13年７月27日(2001.7.27)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｊ	５Ｂ０１７
Ｇ０６Ｆ　12/14		Ｇ０６Ｆ　12/14		５Ｂ０５８
	３２０		３２０Ｃ	

審査請求　未請求　請求項の数３　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－8552(P2000－8552)

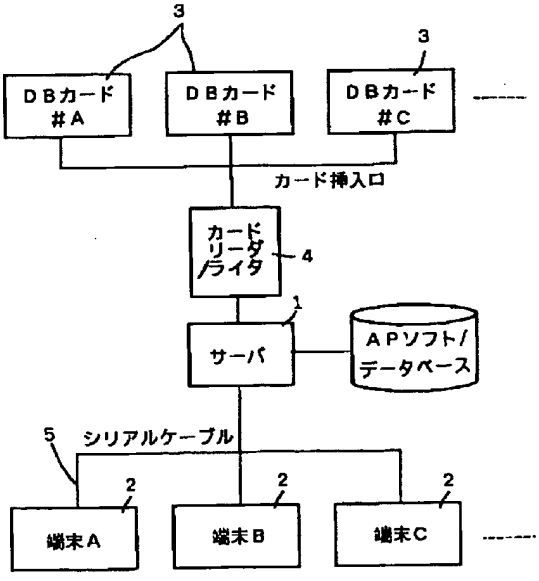
(22)出願日　平成12年１月18日(2000.1.18)

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(72)発明者　大塚　基
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(74)代理人　100073221
弁理士　花輪　義男

Ｆターム(参考)　5B017 AA01 BA05 BA07 BB02 BB06
BB09 CA07 CA08 CA09 CA14
CA16
5B058 KA33 KA35 YA20

(54)【発明の名称】　セキュリティ管理システムおよびそのプログラム記録媒体

(57)【要約】
【課題】サーバ装置がＤＢカードにＤＢファイルを書き込む際に、そのＤＢカードの使用が許可されているユーザのパスワードを暗号化して書き込んで登録しておくが、ユーザパスワードをどのように暗号化するかをその都度変えることで、登録されたユーザパスワードが第三者によって解読される可能性を極力下げることができ、重要情報の漏洩を確実に防止する。
【解決手段】サーバ装置１はＤＢカード３にＤＢファイルを書き込む際に、その都度変化する時間変数をキーとして、ユーザパスワードを暗号化してＤＢカードに登録する。携帯端末装置２は、ＤＢカードに対するアクセス時において、カードから時間変数キーを取得し、オペレータが入力したパスワードをこの時間変数キーによって暗号化してパスワードの照合を行い、正当なユーザであれば、カード内のＤＢファイルに対するアクセスを許可する。



BEST AVAILABLE COPY

1

【特許請求の範囲】

【請求項１】携帯端末装置と、この携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置とを有し、サーバ装置は、データ記憶媒体にデータファイルを書き込む際に、その都度変化する変数を加味して、このデータ記憶媒体を利用することが許可されているユーザの認証情報を暗号化する暗号化手段と、この暗号化手段によって暗号化されたユーザの認証情報をデータ記憶媒体に書き込む書込手段とを具備し、携帯端末装置は、前記変数を加味して、そのオペレータが入力した認証情報を暗号化する暗号化手段と、この暗号化手段によって暗号化されたオペレータの認証情報と前記データ記憶媒体内に暗号化されて記憶されているユーザの認証情報とを照合することにより、正当なユーザかを判別する判別手段と、この判別手段によって正当なユーザであることが判別された際に、前記データ記憶媒体内に書き込まれているデータファイルに対するアクセスを許可するアクセス制御手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項２】前記ユーザの認証情報は、予めサーバ装置側に設定登録されていると共に、当該認証情報自体をキーとして暗号化されており、前記サーバ装置側の暗号化手段は、設定登録されている暗号化認証情報を更に前記変数を加味して暗号化することにより多重暗号化認証情報を生成し、前記携帯端末装置側の暗号化手段は、そのオペレータが入力した認証情報を、当該認証情報自体をキーとして暗号化すると共に、更に前記変数を加味して暗号化することにより多重暗号化認証情報を生成し、前記判別手段は、入力されて多重に暗号化されたオペレータの認証情報と前記データ記憶媒体内に多重に暗号化された状態で記憶されているユーザの認証情報とを照合することにより、正当なユーザかを判別するようにしたことを特徴とする請求項１記載のセキュリティ管理システム。

【請求項３】コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置に対して、データ記憶媒体にデータファイルを書き込む際に、その都度変化する変数を加味して、このデータ記憶媒体を利用することが許可されているユーザの認証情報を暗号化させるコンピュータが読み取り可能なプログラムコードと、暗号化されたユーザの認証情報をデータ記憶媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、携帯端末装置に対して、前記変数を加味して、そのオペレータが入力した認証情報を暗号化させるコンピュータが読み取り可能なプログラムコードと、暗号化されたオペレータの認証情報と前記データ記憶媒体内に暗号化されて記憶されているユーザの認証情報とを照合することにより、正当なユーザかを判別させるコンピュータが読み取り可能なプログラムコードと、正当なユーザであることが判別された際に、前記データ記憶媒体内に書き込まれているデータファイルに対するアクセスを許可させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、携帯端末装置によって可搬型データ記憶媒体をアクセスする際のセキュリティ対策を講じたセキュリティ管理システムおよびそのプログラム記録媒体に関する。

【０００２】

【従来の技術】近年、コンパクトディスクやメモリカード等の可搬型記憶媒体は、大容量化、小型化が進み、大量のデータベースを可搬型記憶媒体に格納することによって、各種のデータベースを自由に持ち運びことができるようになってきている。ここで、営業担当者が携帯端末装置を持参して、日常の営業活動を行う場合において、携帯端末装置はその内蔵メモリの容量が少ないために、各種業務処理用のデータベースの一部あるいは全部を可搬型記憶媒体に格納するようにしている。そして、営業担当者は、端末本体に可搬型記憶媒体を装着し、外出先でその記憶内容をアクセスして表示出力させたり、データ更新等を行うようにしている。この場合、携帯端末装置によって可搬型記憶媒体をアクセスする際のセキュリティ対策としては、入力されたパスワードによって正当な端末利用者かを認証するようにしている。

【０００３】

【発明が解決しようとする課題】ところで、本来、個人専用機としての携帯端末装置においても、正社員の他、派遣社員、パート、アルバイトの方も使用するケースが増えてきている。したがって、可搬型記憶媒体や端末の内蔵メモリ内に、機密性の高い重要な企業情報や個人情報が格納されている場合に、悪意によって、その重要情報が他人に漏洩されるおそれは極めて高かった。すなわち、従来においては、ユーザパスワードを暗号化して記憶しておいたとしても、いつかは暗号化パスワードが解読される危険性があり、派遣社員、パート等による悪意に対するセキュリティ対策は、十分ではなく、重要情報が他人に漏洩されてしまう危険性があった。この発明の課題は、サーバ装置が可搬型データ記憶媒体にデータファイルを書き込む際に、そのデータ記憶媒体の使用が許可されているユーザの認証情報を暗号化して書き込んで登録しておくが、ユーザ認証情報をどのように暗号化するかをその都度変えることで、登録されたユーザ認証情報が第三者によって解読される可能性を極力下げることができ、重要情報の漏洩を防止できるようすることである。

【０００４】この発明の手段は、次の通りである。請求

項第１記載の発明は、携帯端末装置と、この携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置とを有し、サーバ装置は、データ記憶媒体にデータファイルを書き込む際に、その都度変化する変数を加味して、このデータ記憶媒体を利用することが許可されているユーザの認証情報を暗号化する暗号化手段と、この暗号化手段によって暗号化されたユーザの認証情報をデータ記憶媒体に書き込む書込手段とを具備し、携帯端末装置は、前記変数を加味して、そのオペレータが入力した認証情報を暗号化する暗号化手段と、この暗号化手段によって暗号化されたオペレータの認証情報と前記データ記憶媒体内に暗号化されて記憶されているユーザの認証情報とを照合することにより、正当なユーザかを判別する判別手段と、この判別手段によって正当なユーザであることが判別された際に、前記データ記憶媒体内に書き込まれているデータファイルに対するアクセスを許可するアクセス制御手段とを具備するものである。なお、前記ユーザの認証情報は、予めサーバ装置側に設定登録されていると共に、当該認証情報自体をキーとして暗号化されており、前記サーバ装置側の暗号化手段は、設定登録されている暗号化認証情報を更に前記変数を加味して暗号化することにより多重暗号化認証情報を生成し、前記携帯端末装置側の暗号化手段は、そのオペレータが入力した認証情報を、当該認証情報自体をキーとして暗号化すると共に、更に前記変数を加味して暗号化することにより多重暗号化認証情報を生成し、前記判別手段は、入力されて多重に暗号化されたオペレータの認証情報と前記データ記憶媒体内に多重に暗号化された状態で記憶されているユーザの認証情報とを照合することにより、正当なユーザかを判別するようにしてもよい。したがって、請求項第１記載の発明においては、サーバ装置が可搬型データ記憶媒体にデータファイルを書き込む際に、そのデータ記憶媒体の使用が許可されているユーザの認証情報を暗号化して書き込んで登録しておくが、ユーザ認証情報をどのように暗号化するかをその都度変えることで、登録されたユーザ認証情報が第三者によって解読される可能性を極力下げることができ、重要情報の漏洩を防止することができる。

【０００５】

【発明の実施の形態】以下、図１～図１２を参照してこの発明の一実施形態を説明する。図１は、この実施形態におけるセキュリティ管理システムの全体構成を示したブロック図である。このセキュリティ管理システムは、例えば、会社組織において会社側に設置させているサーバ装置１と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末装置）２と、この携帯端末装置２にセットされて利用される可搬型記憶媒体３とを有している。そして、サーバ装置１側で記憶管理されているアプリケーションソフト／データベース等を持ち運び自在な可搬型記憶媒体３を介して携帯端末装置２側に外部提供するようにしており、この記憶媒体３にデータベース等を書き込んで端末装置へ配布する際に、サーバ装置１は当該端末と記憶媒体とを対応付けるための情報を設定したり、各種のセキュリティ対策を講じることによって、記憶媒体３内のアプリケーションソフト／データベース等が第三者によって不正コピーされたり、情報が漏洩されることを確実に防止するようにしたものである。

【０００６】そして、各営業担当者は、外出先で可搬型記憶媒体３内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記憶媒体３を抜き取り、それをサーバ装置１側のカードリーダ／ライタ４にセットすると、サーバ装置１はカードリーダ／ライタ４を介して記憶媒体３内の営業記録を収集処理するようにしている。そして、サーバ装置１と複数台の携帯端末装置２とはシリアルケーブル５を介して着脱自在に接続可能となっている。

【０００７】可搬型記憶媒体３は、各種業務処理用のアプリケーションソフトやデータベース等を記憶するもので、例えば、コンパクトフラッシュカードによって構成されている。以下、可搬型記憶媒体３をデータベースカード（ＤＢカード）と称する。ここで、図中、各ＤＢカード３に付した「＃Ａ」「＃Ｂ」、「＃Ｃ」、‥‥は、端末名称「Ａ」、「Ｂ」、「Ｃ」、‥‥で示される携帯端末装置２に対応付けられた端末対応のカードであることを示している。なお、この実施形態においては端末対応のカードの他、後述する端末グループ対応のカードも存在するが、図１の例では端末対応のカードのみを示している。カードリーダ／ライタ４はＤＢカード３を複数枚同時にセット可能なもので、複数のカード挿入口を有している。そして、サーバ装置１はＤＢカード３を介して携帯端末装置２側にアプリケーションソフト／データベースファイル（ＡＰソフト／ＤＢファイル）を配布する。すなわち、サーバ装置１はＤＢカード３に書き込む書込対象、つまり、配布対象のＡＰソフト／ＤＢファイルを呼び出してカードリーダ／ライタ４に与え、それにセットされている１または２以上のＤＢカード３にＡＰソフト／ＤＢファイルを書き込む。

【０００８】図２は、例えば、業務グループ「営業１課」、「営業２課」、「プロジェクトＡ」、「プロジェクトＢ」、‥‥に対応付けた端末グループと、この端末グループ対応のＤＢカード３との関係を示すと共に、端末とユーザとの対応関係を示したものである。すなわち、図中、「＃Ａ１」、「＃Ａ２」、「＃Ａ３」で示す各ＤＢカード３は、端末名称が「Ａ１」、「Ａ２」、「Ａ３」である各携帯端末装置２が属する端末グループＡ対応の記憶媒体であり、同様に、「＃Ｂ１」、「＃Ｂ２」‥‥で示す各ＤＢカード３は、端末名称が「Ｂ１」、「Ｂ２」、‥‥である各携帯端末装置２が属する

端末グループＢ対応の記憶媒体であり、同一グループ内の各ＤＢカード３はそのグループに属する各携帯端末装置２で共通して使用することができるようになっている。

【０００９】また、ある携帯端末を利用することができる権限を有するユーザは、一人と限らず、複数のユーザが一台の携帯端末装置を共有して使用することができ、また、あるユーザは複数台の携帯端末装置を利用することができる権限を有している。例えば、端末グループＡにおいて、端末名称「Ａ１」で示される携帯端末装置と、ユーザ「ＵＡ１」～「ＵＡ４」との対応関係が定義され、また、端末名称「Ａ２」で示される携帯端末装置と、ユーザ「ＵＡ１」～「ＵＡ３」との対応関係が定義されており、これらの間に限り利用関係があることを示している。この場合、複数ユーザによる共有使用が可能な端末対応の各ＤＢカードには、共有使用が可能な各ユーザに対応して、その認証情報（パスワード）が設定される。

【００１０】図３は、この実施形態におけるセキュリティ管理を概念的に示した図である。すなわち、この実施形態におけるセキュリティ管理として、（Ａ）‥‥ＤＢカードに対するセキュリティ管理、（Ｂ）‥‥パスワード認証によるセキュリティ管理、（Ｃ）‥‥サスペンド／レジューム機能によるセキュリティ管理を行うようにしている。先ず、（Ａ）‥‥ＤＢカードに対するセキュリティ管理について説明する。この実施形態においては、携帯端末装置２が任意のＤＢカードをアクセスする際に、あるいはＤＢカード３が任意の端末装置によってアクセスされる際において、端末およびカード内にそれぞれ記憶されているハード識別番号（後で詳述する）同士を照合し、その照合結果に基づいて当該カード自体に対するアクセス可否を決定するチェック処理を行うようにしている。このチェック処理は端末の電源投入時において、カード内に格納されている基本ソフトの起動によって実行開始される。ここで、「ハード識別番号」は、携帯端末装置２とＤＢカード３とを対応付けておくために予め携帯端末装置２やＤＢカード３に書き込まれたものである。すなわち、サーバ装置１が携帯端末装置２やＤＢカード３へ書き込むための内容を予めテーブル設定しておく際に、「ハード識別番号」は、同一グループに属する携帯端末装置２のうち、いずれか一台の端末から読み込んだ固有の端末識別情報（製造番号）に応じて生成されたもので、サーバ装置１はグループ対応の各携帯端末装置２およびそれらの端末で利用される各ＤＢカード３内に、ハード識別番号をそれぞれ書き込む。したがって、同一グループに属する各携帯端末装置２および各ＤＢカード３内には、それぞれ同一のハード識別番号が共通のアクセス制限情報としてそれぞれ書き込まれる。

【００１１】次に、（Ｂ）‥‥パスワード認証によるセキュリティ管理について説明する。この実施形態においては、上述のＤＢカードセキュリティチェックの結果、当該カード自体に対するアクセスが許可された場合に、入力されたユーザ認証情報（パスワード）に基づいて正当なオペレータかを照合するチェック処理を行うようにしている。この場合の照合には、多重暗号化パスワードが用いられる。すなわち、この多重暗号化パスワードは、入力されたパスワードを所定の方法で2回暗号化した二重暗号化パスワードであり、どのように暗号化するかの具体的な説明は後で詳述するが、この実施形態においては、特に多重暗号化パスワードを常に同じ内容のままとせず、カードへの書込みを行う都度、その内容を変えるようにしている。なお、多重暗号化パスワードはＤＢカード３内にユーザ固有の認証情報としてそれぞれ書き込まれている。この場合、その端末に対してアクセス権限が付与されている複数のユーザが存在している場合には、各ユーザ毎に多重暗号化パスワードの書き込みが行われる。また、ＤＢカード３の利用時において、ユーザパスワードが入力された際に、間違ったパスワードが連続して何回か繰り返して誤入力された場合、その繰り返し入力回数が予め設定されている限度値（後述するビューア不作動設定回数）に達したことが判別されると、それ以降、検索ビューア（パスワード入力を促す表示等の初期画面表示）を不作動とすることにより、パスワード入力を受け付けない状態とするセキュリティ処理も合わせて行うようにしている。

【００１２】更に、（Ｃ）‥‥サスペンド／レジューム機能によるセキュリティ管理について説明する。各携帯端末装置２はサスペンド／レジューム機能を有し、一定時間入力操作が行われないアイドリング状態を監視し、一定時間入力操作が行われなかった場合には、バッテリィ節約やセキュリティ保護のために、現在の状態を退避記憶させたのち、電源をオフしてサスペンド状態となるが、その後の入力操作によってレジューム機能が働き、一定の条件で元の状態に復帰させる。この場合の条件としては、サスペンド時の画面、例えば、アプリケーション画面にそのまま復帰させるのではなく、検索ビューアを作動させてパスワード入力画面を表示させ、再度、パスワードの入力を促し、正当なユーザであることを確認した上で、元の状態、例えば、サスペンド時のアプリケーション画面に復帰させるようにしている。つまり、この実施形態においては、セキュリティ対策のためにレジューム復帰に対して一定の条件を付加し、その条件が成立する場合に限り、サスペンド時の元の状態に復帰させるようにしている。

【００１３】図４（Ａ）は、サーバ装置１側に設けられている設定テーブル１１を示している。この設定テーブル１１はサーバ装置１がＤＢカード３や携帯端末装置２に書き込むための各種の内容を予め設定しておくもので、この実施形態においては、ＤＢカード３への書き込みを携帯端末装置２自体に行わせるのではなく、サーバ

装置１側で一括して行うようにしている。設定テーブル１１はグループ「営業１課」、「営業２課」、「プロジェクトＡ」、「プロジェクトＢ」、‥‥のような端末グループ毎に、各種の設定エリアを有する構成となっている。なお、テーブル設定を行うことができる者は、特別な権限を持った管理者であることは当然であるが、端末グループ毎に管理者を特定しておいてもよい。この場合、グループ管理者は、自己のグループに対してのみ設定の権限を有し、他のグループの設定内容を閲覧することは、勿論禁止される。この各グループ毎の設定エリアにセットされた内容は、当該グループ対応の各携帯端末装置２や各ＤＢカード３内に書き込まれる。なお、図４（Ａ）は、端末グループとして「営業１課」、「営業２課」、「営業１課」を例示した場合を示している。先ず、各グループ対応の設定エリアには「グループ名称」の他、上述した「ハード識別番号」、同一グループに属する端末の合計「設定台数」、同一グループ内のおいて、その端末を使用することができる権限を持つユーザの合計「使用人数」がそれぞれ設定されている。

【００１４】更に、グループ毎に設定されている「ビューア不作動設定回数（Ｎ）」は、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビューアを不作動とするためにグループ毎に任意に設定された設定回数である。また、使用の権限を有する各ユーザに対応付けて、その「ユーザ名（１）」、「暗号化パスワード」、「ユーザ名（２）」、‥‥が設定されている。また、書き込み対象としての「ＢＤファイル名」と、それに対応付けられている「対応ＡＰ（アプリケーション）」が設定されている。「ＤＢファイル名」は、図４（Ｂ）で示すように、サーバ装置側で記憶管理されている複数のマスタＤＢファイル１２のうち、当該グループの業務内容等に応じて必要とするＤＢファイルを指定するものであり、また、「対応ＡＰ」はＢＤファイルを処理するためのアプリケーションソフトであり、マスタＤＢ対応の基本ＡＰ１３（図４（Ｃ）参照）をＢＤファイルに応じてその表示形態を修正変更したものである。

【００１５】一方、設定テーブル１１には、各グループに共通して各ＤＢカードに書き込まれる共通の書き込み対象として、「基本ソフト」がグループ対応設定エリアとは別のエリアに設定されている。ここで、「基本ソフト」には「検索ビューア」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」を含む構成となっている。「基本ソフト」は、携帯端末装置の基本的な動作を実行制御するための基本ソフトであり、「検索ビューア」は基本ソフトの動作に応じて初期画面（ログイン入力画面）を表示させるソフトである。「暗号化／復号化アルゴリズム」はパスワードの暗号化／復号化処理を実行するためのものであり、「動作制御管理ファイル」はＤＢ対応カスタマイズＡＰを動作制御するための基本的な管理情報が格納されているファイルである。この「動作制御管理ファイル」は通常カード内に書き込まれているが、この実施形態においては、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビューアを不作動とするために、「動作制御管理ファイル」を削除するようにしており、検索ビューア起動時に、この「動作制御管理ファイル」がＤＢカード内に存在していることを条件として、携帯端末装置はログイン入力画面を表示させるようにしている。

【００１６】図５は、サーバ装置によって各ＤＢカード３に書き込まれた内容を示している。すなわち、ＤＢカードには、「ハード識別番号」、「基本ソフト」、「検索ビューア」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」、「ビューア不作動設定回数」が書き込まれている。更に、当該ＤＢカードを使用可能な各ユーザに対応して「ユーザ名（１）」、「多重暗号化パスワード＋時間変数キー」、「ユーザ名（２）」‥‥が書き込まれていると共に、「ＤＢファイル」、「対応ＡＰ」が書き込まれている。

【００１７】図６は、各携帯端末装置２の内蔵メモリに書き込まれた内容を示している。この内蔵メモリには、図示のようにフラッシュＲＯＭ、ＲＡＭ設けられている。このＲＯＭ、ＲＡＭは、セキュリティ対策をも考慮して必要最小限のメモリ容量とした構成となっている。すなわち、この実施形態においては、上述のように、アプリケーション、データベース、基本ソフト等の格納場所を携帯端末装置２とＤＢカード３とに分散せず、ＤＢカード３にアプリケーション、データベースの他、基本ソフトをも書き込むようにしており、携帯端末自体の紛失、盗難等によるリスクを解消できるようにしている。ここで、サーバ装置１の書き込み動作によって端末内のフラッシュＲＯＭには、上述した「ハード識別番号」が固定的に記憶される。また、一時記憶メモリであるＲＡＭは、「キー／データ入力エリア」、「レコードエリア」、「その他のワークエリア」を有する構成となっている。なお、「レコードエリア」は端末内にデータを残さないようにするため、必要最小限のデータ、つまり、現在処理中のカレント分として１レコード分のデータを一時記憶する構成となっている。また、電源バックアップによって常時、記憶内容が保障されているＲＡＭには、サスペンド時において、現在の状態が退避される退避データ入力エリアと、サスペンド中であることを示すサスペンドＦ（フラグ）がセットされるフラグエリアが設けられている。なお、図示しないが、各携帯端末装置２の内部メモリには、それが製造された端末固有の製造番号も固定的に記憶されている。

【００１８】図７は、サーバ装置１、携帯端末装置２の全体構成を示したブロック図である。ここで、サーバ装置１、携帯端末装置２の構成要素として基本的に同様なものは、同一番号を付してその説明を兼用するが、サー

バ装置１、携帯端末装置２との構成要素を識別するために、サーバ装置１の構成要素には、図中「Ａ」を付し、以下、携帯端末装置２の構成のみを説明し、サーバ装置１の説明は省略するものとする。ＣＰＵ２１は、記憶装置２２内のオペレーティングシステムや各種アプリケーションソフトにしたがってこの携帯端末装置２の全体動作を制御する中央演算処理装置である。記憶装置２２は、オペレーティングシステムや各種アプリケーションソフトの他、データベース、文字フォント等が格納され、磁気的、光学的、半導体メモリ等によって構成されている記録媒体２３やその駆動系を有している。この記録媒体２３はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なＣＤ－ＲＯＭ、フロッピィディスク、ＲＡＭカード、磁気カード等の可搬型の媒体である。また、この記録媒体２３内のプログラムやデータは、必要に応じてＣＰＵ２１の制御によりＲＡＭ（例えば、スタティクＲＡＭ）２４にロードされたり、ＲＡＭ２４内のデータが記録媒体２３にセーブされる。更に、記録媒体はサーバ等の外部機器側に設けられているものであってもよく、ＣＰＵ２１は伝送媒体を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。また、ＣＰＵ２１は記録媒体２３内に格納されるその一部あるいは全部を他の機器側から伝送媒体を介して取り込み、記録媒体２３に新規登録あるいは追加登録することもできる。すなわち、コンピュータ通信システムを構成する他の機器から通信回線やケーブル等の有線伝送路あるいは電波、マイクロウエーブ、赤外線等の無線伝送路を介して送信されてきたプログラム／データを伝送制御部２５によって受信して記録媒体２３内にインストールすることができる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、ＣＰＵ２１は伝送媒体を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。一方、ＣＰＵ２１にはその入出力周辺デバイスである伝送制御部２５、入力部２６、表示部２７がバスラインを介して接続されており、入出力プログラムにしたがってＣＰＵ２１はそれらの動作を制御する。入力部２６はキーボードやタッチパネルあるいはマウスやタッチ入力ペン等のポインティングデバイスを構成する操作部であり、文字列データや各種コマンドを入力する。

【００１９】次に、この一実施形態におけるセキュリティ管理システムの動作を図８～図１２に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記録媒体２３（２３Ａ）に格納されており、ＣＰＵ２１（２１Ａ）はこのプログラムコードにしたがった動作を逐次実行する。また、ＣＰＵ２１（２１Ａ）は伝送媒体を介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。すなわち、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【００２０】図８および図９は、サーバ装置１が設定テーブル１１に対して各種設定を行う場合の動作を示したフローチャートである。先ず、基本的なグループ情報を設定登録する処理が行われる（ステップＡ１～Ａ９）。ここで、オペレータは入力可能な状態において、今回設定する１グループ分の「グループ名称」を入力指定すると共に（ステップＡ１）、そのグループ内の端末「設定台数」、ユーザ「使用人数」の入力を行う（ステップＡ２）。そして、指定台数分の携帯端末装置２と、その端末に対応付けるＤＢカード３とをサーバ装置１にセットする（ステップＡ３）。すると、サーバ装置１はセットされている同一グループ内の各端末のうち、いずれか１台の端末を選択指定して、その「製造番号」を読み出すと共に（ステップＡ４）、この「製造番号」に基づいて「ハード識別番号」を生成して（ステップＡ５）、設定台数分の各携帯端末装置２およびＤＢカード３に「ハード識別番号」をそれぞれ書き込む（ステップＡ６）。次のステップＡ７では、上述のように入力された「グループ名称」、「設定台数」、「使用人数」の他、生成した「ハード識別番号」を設定テーブル１１にそれぞれ登録する処理が行われる。そして、パスワード不一致でのビューア不作動回数として任意の値をオペレータが入力すると（ステップＡ８）、入力された「ビューア不作動回数」は、設定テーブル１１に登録される（ステップＡ９）。

【００２１】このようにしてグループ基本情報の設定登録が終わると、そのグループの使用人数分のパスワードを設定登録する処理に移る（ステップＡ１０～Ａ１４）。先ず、オペレータはユーザ名を入力すると共に（ステップＡ１０）、そのユーザ対応のパスワードを入力する（ステップＡ１１）。すると、入力されたパスワードは当該パスワード自体をキーとして暗号化される（ステップＡ１２）。そして、入力されたユーザ名、暗号化パスワードは設定テーブル１１にそれぞれ登録される（ステップＡ１３）。これによって一人分のユーザ登録が終わると、使用人数分のユーザ登録が終了したかを調べ（ステップＡ１４）、全ユーザ分の設定が終了するまで上述の動作を繰り返す。

【００２２】そして、ユーザ登録が終了すると、次に、データベースおよびそれに対応するアプリケーションソフトを設定登録する処理に移る（図９のステップＡ１５～Ａ１７）。先ず、オペレータはＤＢカードに書き込むための「ＤＢファイル名」を指定入力すると（ステップＡ１５）、この「ＤＢファイル名」は、設定テーブル１１に登録されると共に（ステップＡ１６）、今回設定登録したＤＢファイル名に対応付けてそのＡＰソフトが設

定テーブル１１に登録される（ステップＡ１７）。次に、全てのグループに対する設定登録が終了したかを調べ（ステップＡ１８）、全グループ終了が判別されるまでステップＡ１に戻り、１グループ毎に上述の動作を繰り返す。これによって設定テーブル１１には、各グループに対応して図４に示した各種の内容が設定登録される。その際、１グループ分の設定登録が終了する毎に、次の設定対象グループを指定して、そのグループ対応の携帯端末装置２、ＤＢカード３をサーバ装置１にセットする。このようなテーブル設定によって携帯端末装置２、ＤＢカード３には「ハード識別番号」がそれぞれ書き込まれる。

【００２３】図１０は、サーバ装置１がＤＢファイルや対応ＡＰソフト等をＤＢカード３に書き込んで配布する場合の動作を示したフローチャートである。先ず、オペレータはサーバ装置１に配布対象のＤＢカード３をセットする（ステップＢ１）。すると、そのカード内から「ハード識別番号」を読み出すと共に（ステップＢ２）、このハード識別番号に基づいて設定テーブル１１を検索し、該当するグループを特定しておく（ステップＢ３）。そして、各グループに共通して各ＤＢカードに書き込まれる共通の書き込み対象としての「基本ソフト」を設定テーブル１１から読み出し、そのＤＢカードに書き込む（ステップＢ４）。この場合、「基本ソフト」には「検索ビューア」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」が含まれているので、それらを含めた書き込みが行われる。次に、特定したグループ対応の「ビューア不作動設定回数（Ｎ）」を設定テーブル１１から読み出してＤＢカードに書き込む（ステップＢ５）。

【００２４】更に、現在のシステム日時を取得し、これを時間変数キーとして特定しておく（ステップＢ６）。そして、特定グループの各ユーザのうち、その先頭のユーザから対応する「暗号化パスワード」を読み出し（ステップＢ７）、上述の時間変数をキーとして、この「暗号化パスワード」を更に暗号化する（ステップＢ８）。これによって生成された多重暗号化パスワードに「時間変数キー」を付加して、対応するユーザ名と共にＤＢカードに書き込む（ステップＢ９）。そして、特定グループの各ユーザを全て指定し終わったかを調べ（ステップＢ１０）、全て指定し終わるまでステップＢ７に戻り、上述の動作を各ユーザ毎に繰り返す。これによって、特定グループの各ユーザ毎にその多重暗号化パスワードとユーザ名をＤＢカードにそれぞれ書き込む処理が終わると、当該グループ対応のＤＢファイル名に基づいて該当するＤＢファイルを読み出し（ステップＢ１１）、カードに書き込むと共に（ステップＢ１２）、そのＤＢファイル対応のＡＰソフトを読み出してカードに書き込む（ステップＢ１３）。

【００２５】図１１および図１２は、携帯端末装置側において電源投入に応じて実行開始されるフローチャートである。先ず、携帯端末装置にＤＢカードがセットされている状態において、電源がオンされると、内蔵メモリであるＲＡＭ内から「サスペンドＦ」を読み出してそれがセットされているかを調べる（ステップＣ１、Ｃ２）。いま、「サスペンドＦ」がセットされていないものとすると、ステップＣ３に移り、ＤＢカード内の基本ソフトに基づいて基本動作が開始される。すると、ＤＢカードから「ハード識別番号」を読み出し（ステップＣ４）、当該端末内の「ハード識別番号」と照合する（ステップＣ５）。この結果、両者が一致する場合には（ステップＣ６）、当該端末とカードとは正当な対応関係にあるので、検索ビューアを起動させるが（ステップＣ９）、当該端末とカードとが正当な対応関係にない場合には、「ハード識別番号」の不一致が判別されるので、ハードエラー表示を行った後（ステップＣ７）、電源を強制的にオフし（ステップＣ８）、エラー終了となる。

【００２６】図１２は、図１１のステップＣ９（検索ビューア起動）時の動作を詳述するためのフローチャートである。先ず、カード内に「動作制御管理ファイル」が存在しているかをチェックする（ステップＤ１）。ここで、上述したように、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビューアを不作動とするために、「動作制御管理ファイル」を削除するようにしている。したがって、「動作制御管理ファイル」の存在有無をチェックし、無ければ、不作動メッセージを表示させる（ステップＤ１０）。そして、「サスペンドＦ」がセットされているかを調べるが（ステップＤ１１）、いま、「サスペンドＦ」はセットされていないので、電源を強制的にオフして（ステップＤ１３）、エラー終了となる。なお、「サスペンドＦ」がセットされていれば、「サスペンドＦ」を含めて各ＲＡＭ内の全データは削除される（ステップＤ１２）。

【００２７】一方、「動作制御管理ファイル」が存在していれば、それを条件としてログイン入力画面を表示させ、ユーザ名、パスワードの入力を促すメッセージを表示する（ステップＤ２）。ここで、オペレータが自己の「ユーザ名」、「パスワード」を入力すると（ステップＤ３）、入力されたパスワードを当該パスワード自体をキーとして暗号化する（ステップＤ４）。そして、ＤＢカード内の当該「ユーザ名」に対応する多重暗号化パスワードに付加されている「時間変数キー」を読み出し、この「時間変数」をキーとして、入力暗号化パスワードを更に暗号化することによって、多重暗号化パスワードを生成する（ステップＤ５）。これによって生成した多重暗号化パスワードとＤＢカードから当該「ユーザ名」に対応して読み出した多重暗号化パスワードとを照合する（ステップＤ６）。

【００２８】その結果、両者の不一致が判別された場合には（ステップＤ７）、その不一致回数を更新すると共

に、その更新値と、予めグループ毎に設定されている「ビューア不作動設定回数（Ｎ）」とを比較し、パスワードの誤入力が連続してＮ回繰り返されたかをチェックし（ステップＤ８）、Ｎ回未満であれば、ログイン入力画面に戻り（ステップＤ２）、その再入力を受け付ける。いま、パスワードの誤入力が連続してＮ回繰り返されたことが判別された場合には（ステップＤ８）、「動作制御管理ファイル」を削除すると共に（ステップＤ９）、不作動メッセージを表示させる（ステップＤ１０）。その後、上述の場合と同様に、「サスペンドＦ」をチェックした後、電源を強制的にオフして、エラー終了となる。

【００２９】また、パスワードの誤入力が連続してＮ回繰り返される前において、パスワードが一致し、正当のオペレータであることが判別された場合には（ステップＤ７）、再び、「サスペンドＦ」のチェックを行うが（ステップＤ１４）、いま、「サスペンドＦ」はセットされていないので、ステップＤ１５に移り、ＤＢファイル名のメニュ画面が一覧表示され、このメニュ画面の中からオペレータが所望するＤＢファイル名を選択指定すると、選択されたＤＢファイル対応のＡＰソフトが起動され（ステップＤ１６）、それに応じたアプリケーション処理が実行される（ステップＤ１７）。この場合、アプリケーション処理の実行中においては、サスペンド機能によって所定時間入力操作が行われないアイドリング状態を監視しており（ステップＤ１８）、アイドリング状態が検出されると、現在、一時記憶メモリにセットされているＲＡＭ内データを退避用のＲＡＭに転送退避すると共に（ステップＤ１９）、「サスペンドＦ」をセットした後（ステップＤ２０）、電源を強制的にオフする（ステップＤ２１）。

【００３０】このようなサスペンド後において、何らかの入力操作が行われると、電源がオンされるので、図１１のフローチャートが実行開始される。この場合、「サスペンドＦ」有りが判別されてステップＤ９に移り、検索ビューアが起動される。この場合、レジューム処理を行う前に、「動作制御管理ファイル」が存在していることを条件としてログイン入力画面を表示させてユーザ名、パスワードの入力を促すメッセージ表示が行われる（ステップＤ２）。ここで、パスワードの一致が検出されて、正当なオペレータであることが判別された場合には（ステップＤ７）、「サスペンドＦ」がセットされていることを条件に、レジューム機能を作動させる（ステップＤ２２）。この場合、サスペンド時のユーザとは異なる他のユーザであっても、カード内に登録されているユーザであれば、正当なオペレータと認識されてレジューム復帰させる。ここで、正当なオペレータであると認識された場合において、ＤＢ選択の初期メニュ画面から始まるのではなく、通常と同様に、サスペンド時の状態に復帰させるために、ＲＡＭ内の退避データを読み出して元の状態であるアプリケーション画面に復帰させる。そして、「サスペンドＦ」を削除した後（ステップＤ２３）、アプリケーション処理に移る（ステップＤ１７）。

【００３１】以上のように、この一実施形態おいて、サーバ装置はＤＢカードにＤＢファイルを書き込む際に、その都度変化する時間変数をキーとして、ユーザパスワードを暗号化してＤＢカードに登録するようにしたから、登録されたユーザパスワードが第三者によって解読される可能性を極力下げることができ、重要情報の漏洩を確実に防止することができる。この場合、ＤＢカードに登録された暗号化パスワードには、その暗号化に使用した時間変数キーが付加されているので、携帯端末装置は、ＤＢカードに対するアクセス時において、カードから時間変数キーを取得し、オペレータが入力したパスワードをこの時間変数キーによって暗号化するようにしたから、暗号用の変数をその都度変化させたとしても、正規なパスワードが入力されれば、登録されているパスワードと同様の暗号結果を得ることができる。したがって、パスワードの照合によって、正当なユーザであれば、ＤＢカード内に書き込まれているＤＢファイルに対するアクセスが許可されるので、ユーザはパスワードがどのように暗号化されているかを全く意識しなくても良く、操作性を妨げることもないことは勿論である。

【００３２】また、ユーザパスワードは、予め当該パスワード自体をキーとして暗号化されてサーバ装置側に設定登録されており、サーバ装置がＤＢファイルをＤＢカードに書き込む際に、その都度変化する時間変数をキーとして、設定登録されている暗号化パスワードを更に暗号化することにより多重暗号化パスワードを生成してカードに書き込むようにしたから、第三者によって解読される可能性を更に下げることができる。

【００３３】一方、任意のＤＢカードをアクセスする際に、このカード内の「ハード識別番号」と自己の「ハード識別番号」とを照合し、その照合結果に基づいて当該カードに対してそのアクセスが許可されている正当な端末であるかをチェックするようにしたから、ＤＢカードを携帯端末装置に装着するだけで自動的にセキュリティ管理が実行されるので、ＤＢカード利用時にユーザはセキュリティ対策を全く意識しなくてもよく、使い勝手を損なわず、確実なセキュリティ管理を実現することができる。この場合、重要情報を含んだＤＢファイルを携帯端末から分離可能なＤＢカードだけに保管しておくようにしたから、携帯端末のみを紛失したり、盗難されたとしてもセキュリティ上全く問題はなく、また、ＤＢカードを紛失したり、盗難された場合でも、そのカードへのアクセスは、正当の端末しかできないようにした仕組みを持っているため、ＤＢファイルに対するアクセスはおろか、ＤＢカード自体に対するアクセスをも不可能となり、そのセキュリティは極めて高いものとなる。

15

【００３４】なお、上述した実施形態においては、ユーザパスワードを当該パスワードをキーとして暗号化したり、時間変数をキーとして暗号化するようにしたが、その暗号化方法は任意であることは勿論であり、また、時間変数キーをカードに書き込むようにしたが、端末側に書き込むようにしてもよい。更に、ユーザパスワードの多重暗号化は二重に限らず、三重以上であってもよい。また、ユーザパスワードを入力して設定テーブルに登録する際に、一回目の暗号化を行い、この暗号化パスワードをカードに書き込む際に、二回目の暗号化を行うようにしたが、パスワードをカードに書き込む際に、一度に多重暗号化パスワードを生成するようにしてもよく、また、多重暗号化パスワードの生成時は任意である。また、「ハード識別番号」をどのような情報に基づいて生成するかは任意であり、例えば、「ハード識別番号」をその携帯端末装置の「製造会社コード」＋「製造番号」等で構成してもよい。また、端末グループは、複数の端末を単に区分けする以外に、1台の端末が複数のグループに属するような設定も可能である。

【００３５】また、上述した一実施形態においては、可搬型記憶媒体であるＤＢカードとして、コンパクトフラッシュカードを例示したが、その他にＰＣカード、スマートメディア、ＣＤ（光ディスク）、ＭＯ（光磁気ディスク）、ＦＤ（フロッピーディスク）等であってもよく、しかも、カード型に限らず、カセット型、スティック型等、その形状は任意である。更に、携帯端末装置としては、電子手帳、ノート型パソコン、ＰＤＡ、携帯電話等であってもよい。

【００３６】

【発明の効果】この発明によれば、サーバ装置が可搬型データ記憶媒体にデータファイルを書き込む際に、そのデータ記憶媒体の使用が許可されているユーザの認証情報を暗号化して書き込んで登録しておくが、ユーザ認証情報をどのように暗号化するかをその都度変えることで、登録されたユーザ認証情報が第三者によって解読される可能性を極力下げることができ、重要情報の漏洩を確実に防止することができる。

【図面の簡単な説明】

【図１】セキュリティ管理システムの全体構成を示したブロック図。

【図２】端末グループ対応のＤＢカード３を説明すると共に、携帯端末装置とユーザとの対応関係を説明するための図。

【図３】セキュリティ管理の種類を概念的に示した図。

【図４】（Ａ）は、サーバ装置側に設けられている設定テーブル１１の構成とその設定内容を示した図、（Ｂ）はマスタＤＢファイル１２を示した図、（Ｃ）はＤＢ対応基本ＡＰ１３を示した図。

【図５】各ＤＢカード３に書き込まれた内容を示した図。

【図６】各携帯端末装置２の内蔵メモリに書き込まれた内容を示した図。

【図７】サーバ装置１、携帯端末装置２の全体構成を示したブロック図。

【図８】サーバ装置１が設定テーブル１１に対して設定を行う場合の動作を示したフローチャート。

【図９】図８に続く設定動作を示したフローチャート。

【図１０】サーバ装置１がマスタＤＢやカスタマイズＡＰ等をＤＢカード３に書き込んで配布する場合の動作を示したフローチャート。

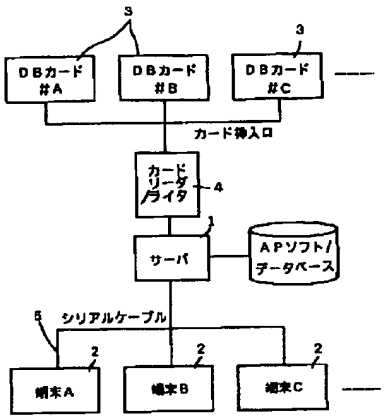
【図１１】携帯端末装置２側において電源投入に応じて実行開始されるフローチャート。

【図12】図１１のステップＣ９（検索ビューア起動）時の動作を詳述するためのフローチャート。

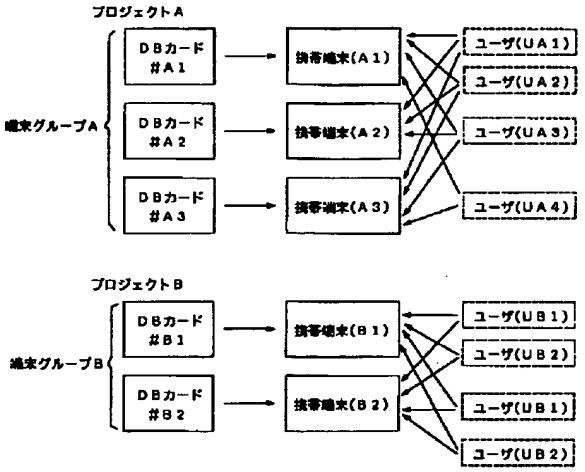
【符号の説明】

１　サーバ装置
２　携帯端末装置
３　ＤＢカード
１１　設定テーブル
１２　マスタＤＢファイル
１３　ＤＢ対応基本ＡＰ
２１、２１Ａ　ＣＰＵ
２２、２２Ａ　記憶装置
２３、２３Ａ　記録媒体
２５、２５Ａ　伝送制御部
２６、２６Ａ　入力部
２７、２７Ａ　表示部

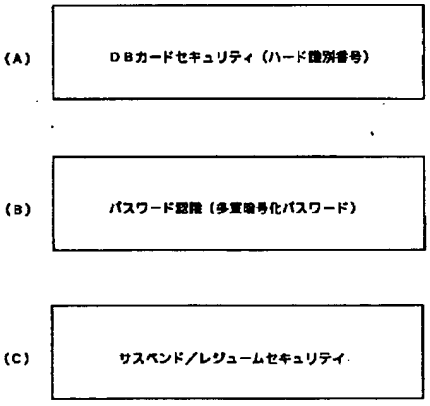
【図１】



【図２】



【図３】



【図４】

サーバ

設定テーブル	グループ	グループ	グループ
グループ名称	営業1課	営業2課	営業3課
ハード識別番号			
設定台数			
使用人数			
ビューア不作動設定回数(N)			
ユーザ名（1）			
暗号化パスワード			
ユーザ名（2）			
暗号化パスワード			
ユーザ名（3）			
暗号化パスワード			
ユーザ名（4）			
暗号化パスワード			
DBファイル名			
対応AP(アプリケーション)			
基本ソフト			
検索ビューア			
暗号化/復合化アルゴリズム			
動作制御管理ファイル			

11

(A)

12

(B) マスタDBファイル （複数）

(C) マスタDB対応の基本AP （複数）

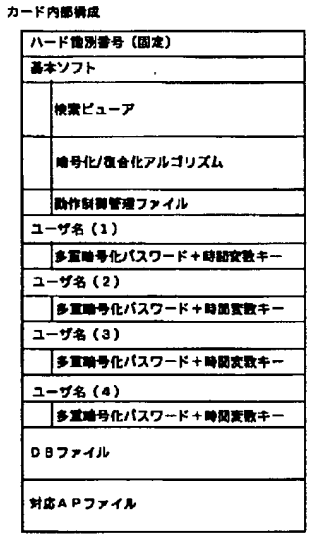
13

【図６】

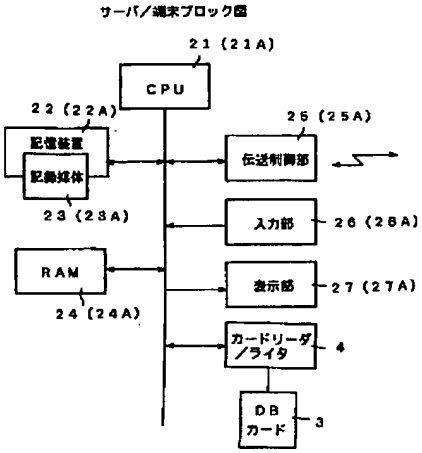
端末内部メモリ構成

FlashROM
ハード識別番号
RAM（一次記憶メモリ）
キー/データ入力エリア
レコードエリア
その他
RAM（電源バックアップ有り）
通過データ入力エリア
サスペンドF

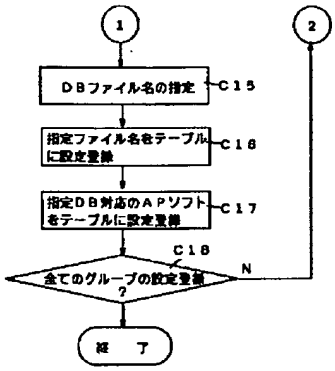
【図５】



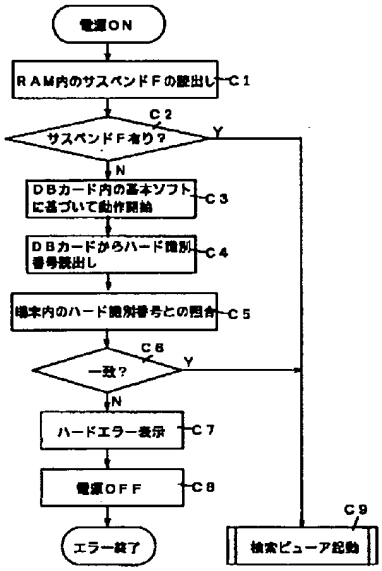
【図７】



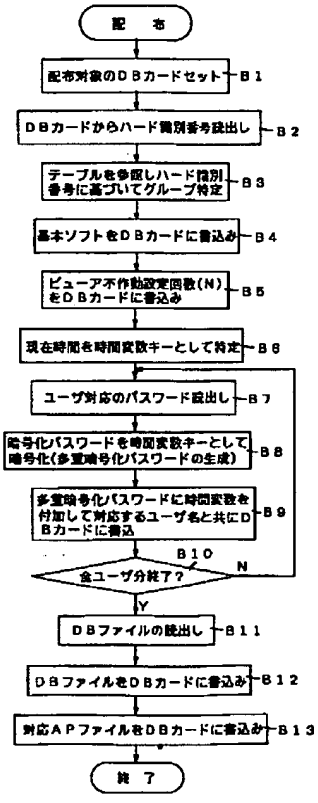
【図９】



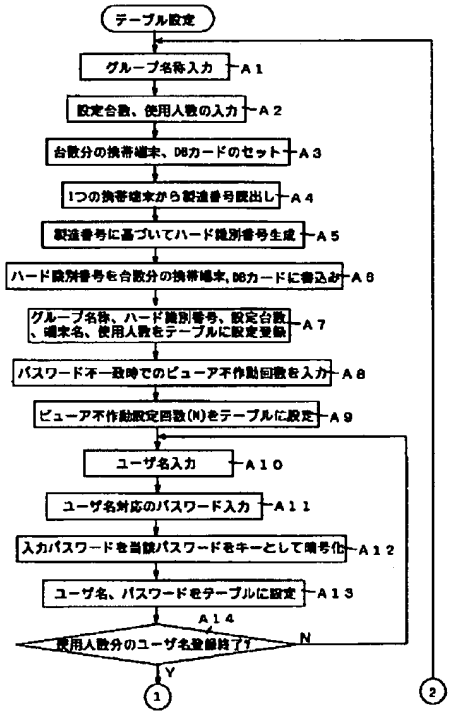
【図１１】



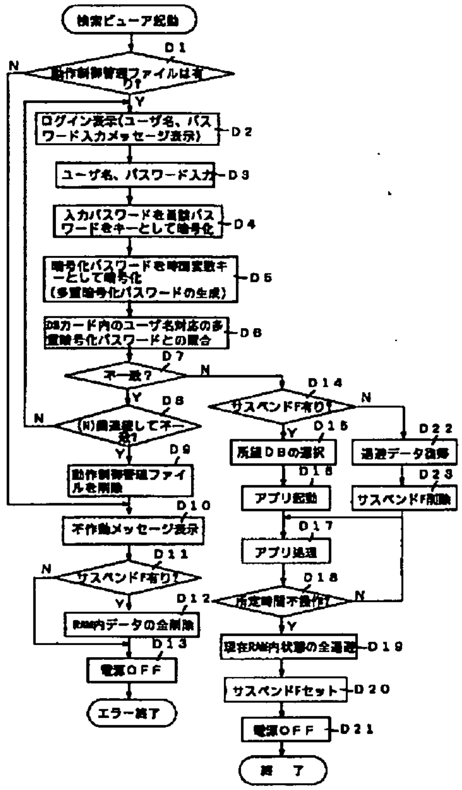
【図１０】



【図８】



【図１２】


検索ビューア起動
D1
動作制御管理ファイルは有り?
N
Y
ログイン表示(ユーザ名、パスワード入力メッセージ表示)
D2
ユーザ名、パスワード入力
D3
入力パスワードを基準パスワードをキーとして暗号化
D4
暗号化パスワードを時間変数キーとして暗号化
(多重暗号化パスワードの生成)
D5
DBカード内のユーザ名対応の多重暗号化パスワードとの照合
D6
不一致?
D7
(N)回連続して不一致?
D8
動作制御管理ファイルを削除
D9
不作動メッセージ表示
D10
サスペンドF有り?
D11
RAM内データの全削除
D12
電源OFF
D13
エラー終了
サスペンドF有り?
D14
所望DBの選択
D15
アプリ起動
D16
アプリ処理
D17
所定時間不操作?
D18
現在RAM内状態の全退避
D19
サスペンドFセット
D20
電源OFF
D21
終了
退避データ復帰
D22
サスペンドF削除
D23

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.